

APPENDIX B-18:

**Invalidity of U.S. Patent No. 7,784,058
by
Choo**

Chart B-18

Invalidity Contentions: Choo

E.D. Tex. Case Nos. 2:24-CV-00093

**Exhibit B-18: Invalidity of U.S. Patent No. 7,784,058
by
Choo**

REFERENCE: U.S. Patent 7,962,950 titled “System and Method for File System Mandatory Access Control” by Tse Huong Choo et al. (hereinafter “Choo”) anticipates and/or renders obvious, including under Plaintiff’s apparent infringement theory,¹ all asserted claims² of U.S. Patent No. 7,784,058 (the “’058 patent”) under 35 U.S.C. §§ 102 and/or 103. Choo published on January 9, 2003 from an application filed on June 29, 2001. Choo is prior art to the ’814 patent under at least 35 U.S.C. §§ 102(a), (e).

The chart below provides representative examples of where each element of each claim is found within Choo, including under Plaintiffs’ apparent construction of the asserted claims (and to the extent the claims are not found indefinite under 35 U.S.C. § 112). The cited evidence is illustrative, and Defendant reserves the right to cite alternative or additional evidence. To the extent Choo does not anticipate any asserted claims or claim elements of the ’058 Patent, Choo nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified herein and/or in HPE’s invalidity contentions cover pleading. To the extent Plaintiff contends that Choo does not disclose any asserted claims or claim elements of the ’058 Patent, it would have been obvious to combine Choo with: (1) the knowledge of one of ordinary skill in the art to show all the limitations of the claims; (2) the teachings of any of the prior art references set forth in Defendant’s other invalidity charts with respect to the one or more limitations; and/or (3) the teachings of any of the prior art references set forth in the cover document of Defendant’s Invalidity Contentions with respect to the ’058 patent. Additionally, to the extent the Choo does not anticipate or render obvious any asserted claims or claim elements of the ’058 Patent, one or more of the prior art materials describing the Choo cited herein individually and/or in combination anticipates and/or renders obvious the asserted claims under 35 U.S.C. §§ 102(a), 102(b), and/or 102(g). Plaintiff has yet to identify any limitation of the asserted claims that it contends is not fully disclosed by Choo, either alone or in combination with other prior art cited by Defendant and/or with the knowledge

¹ To the extent that these Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the Asserted Claims, Defendants are not proposing any such constructions as proper constructions of those terms or phrases. Various positions put forth in this document are predicated on Plaintiff’s incorrect and overly broad interpretation of its claims as evidenced by its Infringement Contentions provided to defendants. Those positions are not intended to and do not necessarily reflect Defendants’ interpretation of the true and proper scope of Plaintiff’s claims, and Defendants reserve the right to adopt claim construction positions that differ from or even conflict with various positions put forth in this document.

² As used herein, “asserted claims” refers only to those claims charted in Plaintiff’s June 5, 2024, Infringement Contentions. To the extent Plaintiff later obtains leave to assert any additional claims for this patent, Defendant will provide its preliminary invalidity contentions consistent with the timing requirements set forth in the Court’s order.

Chart B-18

Invalidity Contentions: Choo

of one of ordinary skill in the art. To the extent Plaintiff makes any such contention in the future, Defendant expressly reserves the right to rebut any such contention, including by identifying additional disclosures and obviousness contentions.

Where the chart below states that Choo “discloses” a limitation, such disclosure may be express or inherent. All emphasis added unless otherwise indicated.

Claim 1

'058 Patent Claim 1	Disclosure
<p>1[p] A computing system for executing a plurality of software applications comprising:</p>	<p>Choo, as evidenced by the example citations below, discloses a computing system for executing a plurality of software applications.</p> <p><i>See, e.g.:</i></p> <ul style="list-style-type: none"> • “When a process attempts to access a particular file, the process performs a system call to the kernel. The identifier of the process is obtained by the kernel routine associated with the system call. The kernel routine accesses the file by reading the list of identifiers. A logical comparison is made between the identifier received from the process and the list of identifiers. If a match is found, the kernel routine performs the access operation (e.g., opening the file). If no match is found, the kernel routine does not perform the access operations and, instead, returns an exception (e.g., error message).” Choo, 1:39-49. • “In one embodiment, the present invention is related to a computer system including compartments implemented on an operating system. A database contains access rules with said access rules defining which compartments are authorized to access particular file resources. A kernel module receives a system call to access a file from a user space application belonging to a compartment. A security module determines whether said user space application is authorized to access said file utilizing access rules stored in said database.” Choo, 2:7-15. • “According to embodiments of the present invention, by utilizing compartments, the security of a computer system may be enhanced through mandatory access control. Mandatory access control refers to access control that a process cannot override. By utilizing mandatory access control, a breach of security in one compartment will not effect resources associated with another compartment. Specifically, if the security of an application operating in compartment A is compromised, the breach of security is limited to a subset of system resources.” Choo, 2:47-56. • “In embodiments of the present invention, any number of system resources may be organized according to compartment access control. For example, system resources associated with TCP/IP networking, routing tables, routing caches, shared memory, message queues, semaphores, process/thread handling, and

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<p>user-id (UID) handling may be limited by utilizing compartments according to embodiments of the present invention.” Choo, 2:66-3:6.</p> <div data-bbox="972 324 1776 745"> <p style="text-align: center;"><i>FIG. 1</i></p> </div> <ul style="list-style-type: none"> “Compartments refer to groups of processes or threads which are limited to accessing certain subsets of system resources of a computer system. FIG. 1 depicts a block diagram example of compartments. This system includes two subsets of system resources (resource 1 and resource 2). This system also includes three compartments (designated compartments A, B, and C). Compartment A is only permitted to access the system resources associated with resource 1. Compartment C is only permitted to access the system resources associated with resource 2. Compartment B is permitted to access the system resources associated with both resource 1 and resource 2. As an example, if a process is designated as belonging to compartment A, the process would be allowed to access resource 1 but would be prevented from accessing resource 2.” Choo, 2:32-46.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="951 264 1791 1060"> </div> <p>FIG. 2</p> <ul style="list-style-type: none"> “FIG. 2 depicts exemplary system 200 that illustrates how compartments may be implemented according to embodiments of the present invention. System 200 includes process 201 that is associated with a compartment. Process 201 executes code in user-space, i.e. a hardware-enforced operating mode that limits the operations of process 201. Process 201 may include code that is operable to attempt to access a protected resource (e.g., opening a certain file) according to a compartment scheme. Process 201 performs a system call to the kernel of the operating system.” Choo, 3:7-16.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="932 261 1808 924"> <p style="text-align: center;">FIG. 3</p> </div> <ul style="list-style-type: none"> <p>“System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system.” Choo, 3:31-46.</p> <p>“SYSTEM compartment 303 may include processes that facilitate command line utilities 304 to modify the compartments or rules associated with the compartments. Command line utilities 304 may include commands to create or delete a particular compartment. Command line utilities 304 may further include commands to create, delete, and/or modify the rules stored in rule database 316 that limit access to system resources.” Choo, 3:47-54.</p>

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Command line utilities 304 may further include commands to execute a process in a specific compartment. For example, a command may be utilized to execute an HTTP web server application in WEB compartment 301. The command causes a thread to be created. The command also creates an entry in the thread registry of the kernel (not shown). The thread is associated with a unique identifier. Also, the thread is associated with the identifier of WEB compartment 301. When the particular thread makes systems calls to the kernel to access system resources, the kernel utilizes the unique thread identifier to determine the compartment identifier. The kernel then determines whether the particular thread is authorized to access the requested resource. It shall be appreciated that this approach is quite advantageous, because this approach requires no modification to the application being executed. Thus, the exemplary compartment approach described herein allows the security of ordinary platforms to be upgraded to include access control without requiring appreciable modification of user-space application code.” Choo, 3:55-4:6. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
1[a] a) a processor;	<p>Choo, as evidenced by the example citations below, discloses a processor.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[p].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
1[b] b) an operating system having an operating system kernel having OS critical system elements (OSCSEs) for running in kernel mode using said processor; and,	<p>Choo, as evidenced by the example citations below, discloses an operating system having an operating system kernel having OS critical system elements (OSCSEs) for running in kernel mode using said processor.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[p].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
<p>1[c] c) a shared library having shared library critical system elements (SLCSEs) stored therein for use by the plurality of software applications in user mode and</p>	<p>Choo, as evidenced by the example citations below, discloses a shared library having shared library critical system elements (SLCSEs) stored therein for use by the plurality of software applications in user mode.</p> <p><i>See, e.g.:</i></p> <ul style="list-style-type: none"> • “One aspect of containment is restricting access to files. For example, it may be advantageous to restrict access to a configuration file, since the configuration file may be utilized to breach the security of the system. Likewise, it is advantageous to prevent most processes from being able to read or write to files containing password information.” Choo, 1:27-32. • “When a process attempts to access a particular file, the process performs a system call to the kernel. The identifier of the process is obtained by the kernel routine associated with the system call. The kernel routine accesses the file by reading the list of identifiers. A logical comparison is made between the identifier received from the process and the list of identifiers. If a match is found, the kernel routine performs the access operation (e.g., opening the file). If no match is found, the kernel routine does not perform the access operations and, instead, returns an exception (e.g., error message).” Choo, 1:39-49. • “In one embodiment, the present invention is related to a computer system including compartments implemented on an operating system. A database contains access rules with said access rules defining which compartments are authorized to access particular file resources. A kernel module receives a system call to access a file from a user space application belonging to a compartment. A security module determines whether said user space application is authorized to access said file utilizing access rules stored in said database.” Choo, 2:7-15. • “According to embodiments of the present invention, by utilizing compartments, the security of a computer system may be enhanced through mandatory access control. Mandatory access control refers to access control that a process cannot override. By utilizing mandatory access control, a breach of security in one compartment will not effect resources associated with another compartment. Specifically, if the security of an application operating in compartment A is compromised, the breach of security is limited to a subset of system resources.” Choo, 2:47-56. • “In embodiments of the present invention, any number of system resources may be organized according to compartment access control. For example, system resources associated with TCP/IP networking, routing tables, routing caches, shared memory, message queues, semaphores, process/thread handling, and user-id (UID) handling may be limited by utilizing compartments according to embodiments of the present invention.” Choo, 2:66-3:6.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="972 264 1776 686"> <p style="text-align: center;"><i>FIG. 1</i></p> </div> <ul style="list-style-type: none"> • “Compartments refer to groups of processes or threads which are limited to accessing certain subsets of system resources of a computer system. FIG. 1 depicts a block diagram example of compartments. This system includes two subsets of system resources (resource 1 and resource 2). This system also includes three compartments (designated compartments A, B, and C). Compartment A is only permitted to access the system resources associated with resource 1. Compartment C is only permitted to access the system resources associated with resource 2. Compartment B is permitted to access the system resources associated with both resource 1 and resource 2. As an example, if a process is designated as belonging to compartment A, the process would be allowed to access resource 1 but would be prevented from accessing resource 2.” Choo, 2:32-46.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="951 266 1791 1060"> <p style="text-align: center;"><i>FIG. 2</i></p> </div> <ul style="list-style-type: none"> “FIG. 2 depicts exemplary system 200 that illustrates how compartments may be implemented according to embodiments of the present invention. System 200 includes process 201 that is associated with a compartment. Process 201 executes code in user-space, i.e. a hardware-enforced operating mode that limits the operations of process 201. Process 201 may include code that is operable to attempt to access a protected resource (e.g., opening a certain file) according to a compartment scheme. Process 201 performs a system call to the kernel of the operating system.” Choo, 3:7-16.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="932 261 1808 927"> <p style="text-align: center;">FIG. 3</p> </div> <ul style="list-style-type: none"> • “System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system.” Choo, 3:31-46. • “SYSTEM compartment 303 may include processes that facilitate command line utilities 304 to modify the compartments or rules associated with the compartments. Command line utilities 304 may include commands to create or delete a particular compartment. Command line utilities 304 may further include commands to create, delete, and/or modify the rules stored in rule database 316 that limit access to system resources.” Choo, 3:47-54.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Command line utilities 304 may further include commands to execute a process in a specific compartment. For example, a command may be utilized to execute an HTTP web server application in WEB compartment 301. The command causes a thread to be created. The command also creates an entry in the thread registry of the kernel (not shown). The thread is associated with a unique identifier. Also, the thread is associated with the identifier of WEB compartment 301. When the particular thread makes systems calls to the kernel to access system resources, the kernel utilizes the unique thread identifier to determine the compartment identifier. The kernel then determines whether the particular thread is authorized to access the requested resource. It shall be appreciated that this approach is quite advantageous, because this approach requires no modification to the application being executed. Thus, the exemplary compartment approach described herein allows the security of ordinary platforms to be upgraded to include access control without requiring appreciable modification of user-space application code.” Choo, 3:55-4:6. • “command line utilities 304 access the kernel via kernel modules 322. Routines of kernel modules 322 advantageously perform the actual manipulation (e.g., addition, modification, or deletion) of the respective objects as desired by the particular commands.” Choo, 4:7-11. • “The kernel of system 300 includes a plurality of modules. Certain modules are accessed by the various compartments via system calls. For example, processes operating in either WEB compartment 301 or FTP compartment 302 may communicate with processes operating on other systems via the Internet by utilizing system calls to routines of TCP/IP networking module 306. Socket communication may occur via UNIX domain sockets module 308. Interprocess communication module 310 includes kernel routines to facilitate communication between processes via shared memory, stacks, semaphores, and/or the like. Interprocess communication module 310 may also facilitate spawning or forking new processes. File access module 312 may facilitate access to files on a file system. For example, file access module 312 may facilitate opening, closing, reading from, writing to, deleting, renaming files, and/or the like.” Choo, 4:19-34. • “As another example, system call wrapping may be utilized. In system call wrapping, wrapper functions, using a dynamically linked shared library, examine system calls and arguments. The wrapper functions also either allow or disallow system calls according to rules defined in a rule database. User-level authorization servers may be utilized to control access to system resources. User-level authorization servers may control access to system resources by providing a controlled data channel to the kernel.” Choo, 4:61-5:3.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="926 264 1818 816"> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “In embodiments of the present invention, access to files by processes is restricted by rules based on process compartments. Reference is now made to FIG. 4 that depicts an exemplary file system to which access is controlled by rules based on process compartments. This file system is organized according to a subdirectory structure. The highest component of this file system is the root directory (referred to as root 401). Underneath root 401, several subdirectories are shown including /apache 402, /lib 403, /etc 404.” Choo, 5:4-12. • “The pathname and filename may be passed to a function or a system call to perform various access operations such as opening the file, reading from the file, writing to the file, renaming the file, deleting the file, and/or the like.” Choo, 5: 21-25. • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
<p>1[d][1] i) wherein some of the SLCSEs stored in the shared library are functional replicas of OSCSEs and are accessible to some of the plurality of software applications and</p>	<p>Choo, as evidenced by the example citations below, discloses that some of the SLCSEs stored in the shared library are functional replicas of OSCSEs and are accessible to some of the plurality of software applications.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c]. <i>E.g.</i>:</p> <div data-bbox="926 760 1818 1312" data-label="Diagram"> <pre> graph TD 401["/(ROOT)"] --> 402["/APACHE"] 401 --> 403["/LIB"] 401 --> 404["/ETC"] 402 --> 405["CONF"] 402 --> 406["LOGS"] </pre> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<p>may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system." Choo, 5:54-67.</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.</p>
<p>1[d][2] when one of the SLCSEs is accessed by one or more of the plurality of software applications it forms a part of the one or more of the plurality of software applications,</p>	<p>Choo, as evidenced by the example citations below, discloses when one of the SLCSEs is accessed by one or more of the plurality of software applications it forms a part of the one or more of the plurality of software applications.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c]. <i>E.g.</i>:</p> <ul style="list-style-type: none"> • "System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system." Choo, 3:31-46.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="926 264 1818 816"> <pre> graph TD 401["/(ROOT)"] --> 402["/APACHE"] 401 --> 403["/LIB"] 401 --> 404["/ETC"] 402 --> 405["CONF"] 402 --> 406["LOGS"] </pre> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67. • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in</p>

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.
<p>1[e][1] ii) wherein an instance of a SLCSE provided to at least a first of the plurality of software applications from the shared library is run in a context of said at least first of the plurality of software applications without being shared with other of the plurality of software applications and</p>	<p>Choo, as evidenced by the example citations below, discloses wherein an instance of a SLCSE provided to at least a first of the plurality of software applications from the shared library is run in a context of said at least first of the plurality of software applications without being shared with other of the plurality of software applications.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c]. <i>E.g.</i>:</p> <div data-bbox="972 527 1776 948"> <pre> graph BT A[COMPARTMENT A] --> R1[RESOURCE 1] B[COMPARTMENT B] --> R1 B --> R2[RESOURCE 2] C[COMPARTMENT C] --> R2 </pre> <p style="text-align: center;"><i>FIG. 1</i></p> </div> <ul style="list-style-type: none"> “Compartments refer to groups of processes or threads which are limited to accessing certain subsets of system resources of a computer system. FIG. 1 depicts a block diagram example of compartments. This system includes two subsets of system resources (resource 1 and resource 2). This system also includes three compartments (designated compartments A, B, and C). Compartment A is only permitted to access the system resources associated with resource 1. Compartment C is only permitted to access the system resources associated with resource 2. Compartment B is permitted to access the system resources associated with both resource 1 and resource 2. As an example, if a process is designated as belonging to compartment A, the process would be allowed to access resource 1 but would be prevented from accessing resource 2.” Choo, 2:32-46.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="951 266 1791 1060"> <p style="text-align: center;"><i>FIG. 2</i></p> </div> <ul style="list-style-type: none"> “FIG. 2 depicts exemplary system 200 that illustrates how compartments may be implemented according to embodiments of the present invention. System 200 includes process 201 that is associated with a compartment. Process 201 executes code in user-space, i.e. a hardware-enforced operating mode that limits the operations of process 201. Process 201 may include code that is operable to attempt to access a protected resource (e.g., opening a certain file) according to a compartment scheme. Process 201 performs a system call to the kernel of the operating system.” Choo, 3:7-16.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="932 261 1808 927"> <p style="text-align: center;">FIG. 3</p> </div> <ul style="list-style-type: none"> • “System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system.” Choo, 3:31-46. • “SYSTEM compartment 303 may include processes that facilitate command line utilities 304 to modify the compartments or rules associated with the compartments. Command line utilities 304 may include commands to create or delete a particular compartment. Command line utilities 304 may further include commands to create, delete, and/or modify the rules stored in rule database 316 that limit access to system resources.” Choo, 3:47-54.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Command line utilities 304 may further include commands to execute a process in a specific compartment. For example, a command may be utilized to execute an HTTP web server application in WEB compartment 301. The command causes a thread to be created. The command also creates an entry in the thread registry of the kernel (not shown). The thread is associated with a unique identifier. Also, the thread is associated with the identifier of WEB compartment 301. When the particular thread makes systems calls to the kernel to access system resources, the kernel utilizes the unique thread identifier to determine the compartment identifier. The kernel then determines whether the particular thread is authorized to access the requested resource. It shall be appreciated that this approach is quite advantageous, because this approach requires no modification to the application being executed. Thus, the exemplary compartment approach described herein allows the security of ordinary platforms to be upgraded to include access control without requiring appreciable modification of user-space application code.” Choo, 3:55-4:6. • “command line utilities 304 access the kernel via kernel modules 322. Routines of kernel modules 322 advantageously perform the actual manipulation (e.g., addition, modification, or deletion) of the respective objects as desired by the particular commands.” Choo, 4:7-11. • “The kernel of system 300 includes a plurality of modules. Certain modules are accessed by the various compartments via system calls. For example, processes operating in either WEB compartment 301 or FTP compartment 302 may communicate with processes operating on other systems via the Internet by utilizing system calls to routines of TCP/IP networking module 306. Socket communication may occur via UNIX domain sockets module 308. Interprocess communication module 310 includes kernel routines to facilitate communication between processes via shared memory, stacks, semaphores, and/or the like. Interprocess communication module 310 may also facilitate spawning or forking new processes. File access module 312 may facilitate access to files on a file system. For example, file access module 312 may facilitate opening, closing, reading from, writing to, deleting, renaming files, and/or the like.” Choo, 4:19-34. • “As another example, system call wrapping may be utilized. In system call wrapping, wrapper functions, using a dynamically linked shared library, examine system calls and arguments. The wrapper functions also either allow or disallow system calls according to rules defined in a rule database. User-level authorization servers may be utilized to control access to system resources. User-level authorization servers may control access to system resources by providing a controlled data channel to the kernel.” Choo, 4:61-5:3.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="926 264 1818 816"> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “In embodiments of the present invention, access to files by processes is restricted by rules based on process compartments. Reference is now made to FIG. 4 that depicts an exemplary file system to which access is controlled by rules based on process compartments. This file system is organized according to a subdirectory structure. The highest component of this file system is the root directory (referred to as root 401). Underneath root 401, several subdirectories are shown including /apache 402, /lib 403, /etc 404.” Choo, 5:4-12. • “The pathname and filename may be passed to a function or a system call to perform various access operations such as opening the file, reading from the file, writing to the file, renaming the file, deleting the file, and/or the like.” Choo, 5: 21-25. • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
<p>1[e][2] where at least a second of the plurality of software applications running under the operating system have use of a unique instance of a corresponding critical system element for performing same function, and</p>	<p>Choo, as evidenced by the example citations below, discloses where at least a second of the plurality of software applications running under the operating system have use of a unique instance of a corresponding critical system element for performing same function.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c]. <i>E.g.</i>:</p> <div data-bbox="968 776 1776 1198" data-label="Diagram"> <pre> graph BT A[COMPARTMENT A] --> R1[RESOURCE 1] B[COMPARTMENT B] --> R2[RESOURCE 2] C[COMPARTMENT C] --> R2 </pre> <p style="text-align: center;"><i>FIG. 1</i></p> </div> <ul style="list-style-type: none"> • “Compartments refer to groups of processes or threads which are limited to accessing certain subsets of system resources of a computer system. FIG. 1 depicts a block diagram example of compartments. This system includes two subsets of system resources (resource 1 and resource 2). This system also includes three compartments (designated compartments A, B, and C). Compartment A is only permitted to access the system resources associated with resource 1. Compartment C is only permitted to access the system resources associated with resource 2. Compartment B is permitted to access the system resources associated with both resource 1 and resource 2. As an example, if a process is designated as belonging to compartment

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<p>A, the process would be allowed to access resource 1 but would be prevented from accessing resource 2.” Choo, 2:32-46.</p> <div data-bbox="951 342 1791 1138"> </div> <ul style="list-style-type: none"> “FIG. 2 depicts exemplary system 200 that illustrates how compartments may be implemented according to embodiments of the present invention. System 200 includes process 201 that is associated with a compartment. Process 201 executes code in user-space, i.e. a hardware-enforced operating mode that limits the operations of process 201. Process 201 may include code that is operable to attempt to access a protected resource (e.g., opening a certain file) according to a compartment scheme. Process 201 performs a system call to the kernel of the operating system.” Choo, 3:7-16.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="932 261 1808 927"> <p style="text-align: center;">FIG. 3</p> </div> <ul style="list-style-type: none"> • “System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system.” Choo, 3:31-46. • “SYSTEM compartment 303 may include processes that facilitate command line utilities 304 to modify the compartments or rules associated with the compartments. Command line utilities 304 may include commands to create or delete a particular compartment. Command line utilities 304 may further include commands to create, delete, and/or modify the rules stored in rule database 316 that limit access to system resources.” Choo, 3:47-54.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Command line utilities 304 may further include commands to execute a process in a specific compartment. For example, a command may be utilized to execute an HTTP web server application in WEB compartment 301. The command causes a thread to be created. The command also creates an entry in the thread registry of the kernel (not shown). The thread is associated with a unique identifier. Also, the thread is associated with the identifier of WEB compartment 301. When the particular thread makes systems calls to the kernel to access system resources, the kernel utilizes the unique thread identifier to determine the compartment identifier. The kernel then determines whether the particular thread is authorized to access the requested resource. It shall be appreciated that this approach is quite advantageous, because this approach requires no modification to the application being executed. Thus, the exemplary compartment approach described herein allows the security of ordinary platforms to be upgraded to include access control without requiring appreciable modification of user-space application code.” Choo, 3:55-4:6. • “command line utilities 304 access the kernel via kernel modules 322. Routines of kernel modules 322 advantageously perform the actual manipulation (e.g., addition, modification, or deletion) of the respective objects as desired by the particular commands.” Choo, 4:7-11. • “The kernel of system 300 includes a plurality of modules. Certain modules are accessed by the various compartments via system calls. For example, processes operating in either WEB compartment 301 or FTP compartment 302 may communicate with processes operating on other systems via the Internet by utilizing system calls to routines of TCP/IP networking module 306. Socket communication may occur via UNIX domain sockets module 308. Interprocess communication module 310 includes kernel routines to facilitate communication between processes via shared memory, stacks, semaphores, and/or the like. Interprocess communication module 310 may also facilitate spawning or forking new processes. File access module 312 may facilitate access to files on a file system. For example, file access module 312 may facilitate opening, closing, reading from, writing to, deleting, renaming files, and/or the like.” Choo, 4:19-34. • “As another example, system call wrapping may be utilized. In system call wrapping, wrapper functions, using a dynamically linked shared library, examine system calls and arguments. The wrapper functions also either allow or disallow system calls according to rules defined in a rule database. User-level authorization servers may be utilized to control access to system resources. User-level authorization servers may control access to system resources by providing a controlled data channel to the kernel.” Choo, 4:61-5:3.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="926 264 1818 816"> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “In embodiments of the present invention, access to files by processes is restricted by rules based on process compartments. Reference is now made to FIG. 4 that depicts an exemplary file system to which access is controlled by rules based on process compartments. This file system is organized according to a subdirectory structure. The highest component of this file system is the root directory (referred to as root 401). Underneath root 401, several subdirectories are shown including /apache 402, /lib 403, /etc 404.” Choo, 5:4-12. • “The pathname and filename may be passed to a function or a system call to perform various access operations such as opening the file, reading from the file, writing to the file, renaming the file, deleting the file, and/or the like.” Choo, 5: 21-25. • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
<p>1[f][1] iii) wherein a SLCSE related to a predetermined function is provided to the first of the plurality of software applications for running a first instance of the SLCSE, and</p>	<p>Choo, as evidenced by the example citations below, discloses wherein a SLCSE related to a predetermined function is provided to the first of the plurality of software applications for running a first instance of the SLCSE.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c]. <i>E.g.</i>:</p> <div data-bbox="972 792 1776 1214" data-label="Diagram"> <pre> graph BT A[COMPARTMENT A] --> R1[RESOURCE 1] B[COMPARTMENT B] --> R1 B --> R2[RESOURCE 2] C[COMPARTMENT C] --> R2 </pre> <p style="text-align: center;"><i>FIG. 1</i></p> </div> <ul style="list-style-type: none"> • “Compartments refer to groups of processes or threads which are limited to accessing certain subsets of system resources of a computer system. FIG. 1 depicts a block diagram example of compartments. This system includes two subsets of system resources (resource 1 and resource 2). This system also includes three compartments (designated compartments A, B, and C). Compartment A is only permitted to access the system resources associated with resource 1. Compartment C is only permitted to access the system resources associated with resource 2. Compartment B is permitted to access the system resources associated

Chart B-18

Invalidity Contentions: Choo

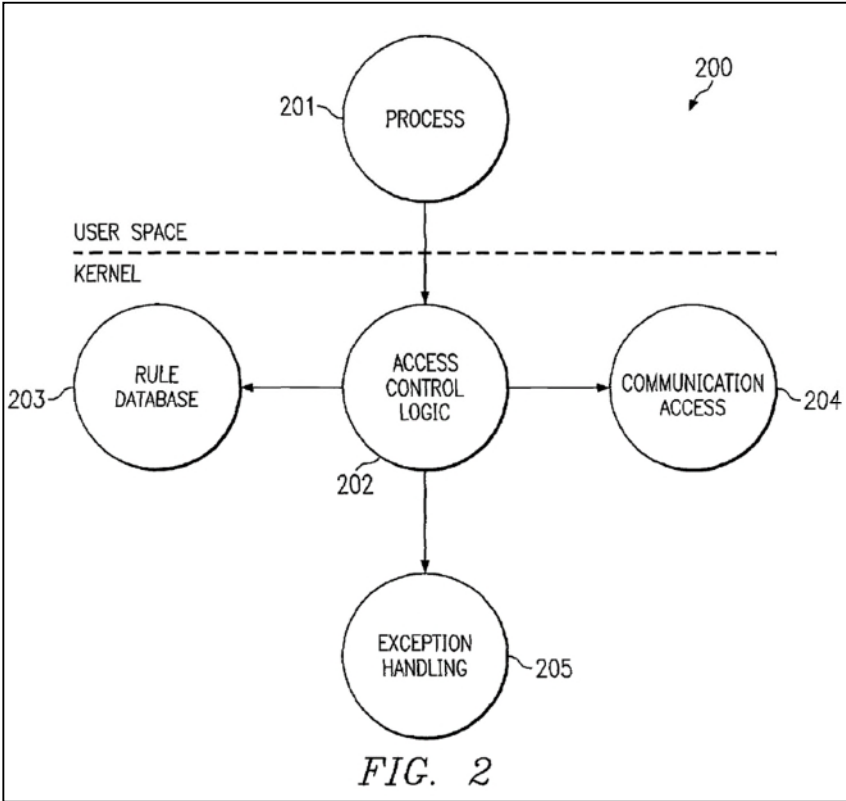
'058 Patent Claim 1	Disclosure
	<p>with both resource 1 and resource 2. As an example, if a process is designated as belonging to compartment A, the process would be allowed to access resource 1 but would be prevented from accessing resource 2.” Choo, 2:32-46.</p>  <p>FIG. 2</p> <ul style="list-style-type: none"> “FIG. 2 depicts exemplary system 200 that illustrates how compartments may be implemented according to embodiments of the present invention. System 200 includes process 201 that is associated with a compartment. Process 201 executes code in user-space, i.e. a hardware-enforced operating mode that limits the operations of process 201. Process 201 may include code that is operable to attempt to access a protected resource (e.g., opening a certain file) according to a compartment scheme. Process 201 performs a system call to the kernel of the operating system.” Choo, 3:7-16.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="932 261 1808 927"> <p style="text-align: center;">FIG. 3</p> </div> <ul style="list-style-type: none"> • “System 300 of FIG. 3 depicts another exemplary system that utilizes compartments to provide containment. System 300 includes a plurality of compartments. In this example, WEB compartment 301, FTP compartment 302, and SYSTEM compartment 303 are shown. Each compartment is associated with various executing processes or threads. The processes of the compartments are limited to accessing system resources according to the rules stored in rule database 316. Rule database 316 may include various components or modules for the various types of resources. Rule database 316 may comprise separate tables for TCP/IP networking resource rules and for file system resource rules. Also, the various components may be stored in different locations. For example, TCP/IP resource rules may be stored in random access memory while file system resource rules may be stored on the file system.” Choo, 3:31-46. • “SYSTEM compartment 303 may include processes that facilitate command line utilities 304 to modify the compartments or rules associated with the compartments. Command line utilities 304 may include commands to create or delete a particular compartment. Command line utilities 304 may further include commands to create, delete, and/or modify the rules stored in rule database 316 that limit access to system resources.” Choo, 3:47-54.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Command line utilities 304 may further include commands to execute a process in a specific compartment. For example, a command may be utilized to execute an HTTP web server application in WEB compartment 301. The command causes a thread to be created. The command also creates an entry in the thread registry of the kernel (not shown). The thread is associated with a unique identifier. Also, the thread is associated with the identifier of WEB compartment 301. When the particular thread makes systems calls to the kernel to access system resources, the kernel utilizes the unique thread identifier to determine the compartment identifier. The kernel then determines whether the particular thread is authorized to access the requested resource. It shall be appreciated that this approach is quite advantageous, because this approach requires no modification to the application being executed. Thus, the exemplary compartment approach described herein allows the security of ordinary platforms to be upgraded to include access control without requiring appreciable modification of user-space application code.” Choo, 3:55-4:6. • “command line utilities 304 access the kernel via kernel modules 322. Routines of kernel modules 322 advantageously perform the actual manipulation (e.g., addition, modification, or deletion) of the respective objects as desired by the particular commands.” Choo, 4:7-11. • “The kernel of system 300 includes a plurality of modules. Certain modules are accessed by the various compartments via system calls. For example, processes operating in either WEB compartment 301 or FTP compartment 302 may communicate with processes operating on other systems via the Internet by utilizing system calls to routines of TCP/IP networking module 306. Socket communication may occur via UNIX domain sockets module 308. Interprocess communication module 310 includes kernel routines to facilitate communication between processes via shared memory, stacks, semaphores, and/or the like. Interprocess communication module 310 may also facilitate spawning or forking new processes. File access module 312 may facilitate access to files on a file system. For example, file access module 312 may facilitate opening, closing, reading from, writing to, deleting, renaming files, and/or the like.” Choo, 4:19-34. • “As another example, system call wrapping may be utilized. In system call wrapping, wrapper functions, using a dynamically linked shared library, examine system calls and arguments. The wrapper functions also either allow or disallow system calls according to rules defined in a rule database. User-level authorization servers may be utilized to control access to system resources. User-level authorization servers may control access to system resources by providing a controlled data channel to the kernel.” Choo, 4:61-5:3.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<div data-bbox="926 264 1818 816"> <p style="text-align: right;"><i>FIG. 4</i></p> </div> <ul style="list-style-type: none"> • “In embodiments of the present invention, access to files by processes is restricted by rules based on process compartments. Reference is now made to FIG. 4 that depicts an exemplary file system to which access is controlled by rules based on process compartments. This file system is organized according to a subdirectory structure. The highest component of this file system is the root directory (referred to as root 401). Underneath root 401, several subdirectories are shown including /apache 402, /lib 403, /etc 404.” Choo, 5:4-12. • “The pathname and filename may be passed to a function or a system call to perform various access operations such as opening the file, reading from the file, writing to the file, renaming the file, deleting the file, and/or the like.” Choo, 5: 21-25. • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67.

Chart B-18

Invalidity Contentions: Choo

'058 Patent Claim 1	Disclosure
	<ul style="list-style-type: none"> • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>
<p>1[f][2] wherein a SLCSE for performing a same function is provided to the second of the plurality of software applications for running a second instance of the SLCSE simultaneously.</p>	<p>Choo, as evidenced by the example citations below, discloses wherein a SLCSE for performing a same function is provided to the second of the plurality of software applications for running a second instance of the SLCSE simultaneously.</p> <p>This element is satisfied by the disclosures set forth in claim element 1[c], [f][1]. <i>E.g.</i>:</p> <ul style="list-style-type: none"> • “For example, database 316 may include a series of data structures for each subdirectory of file system 300. The data structures for each subdirectory may contain the rules pertaining to the respective subdirectories. Also, the data structures may form a linked list structure. Specifically, the data structures may contain a pointer to its parent subdirectory and a pointer to each child subdirectory. By organizing the rules in this preferable manner, security module 320 may search the database in an efficient manner by traversing the data structures according to the pathname of the file to be accessed. It shall be appreciated that other mechanisms may be utilized in lieu of a pointer approach. For example, a relational database structure may be utilized to organize rules according to the structure of the file system.” Choo, 5:54-67. • “Synchronization issues are significantly reduced, since access information need not be modified for each additional or deleted file.” Choo, 6:61-63. • “Accordingly, embodiments of the present invention allow platforms to implement security procedures without requiring modification of the user-space applications or modification of their file systems.” Choo, 7:5-11. <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant’s other invalidity charts for the ’058 patent with respect to this limitation, as described in Defendant’s Invalidity Contentions.</p>

Chart B-18

Invalidity Contentions: Choo

Claim 2

'058 Patent Claim 2	Disclosure
2. A computing system as defined in claim 1, wherein in operation, multiple instances of an SLCSE stored in the shared library run simultaneously within the operating system.	<p>Choo, as evidenced by the example citations below, discloses the computing system as defined in claim 1, wherein in operation, multiple instances of an SLCSE stored in the shared library run simultaneously within the operating system.</p> <p>This element is satisfied by the disclosure set forth at claim element 1[c], [f][1]-[2].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.</p>

Chart B-18

Invalidity Contentions: Choo

Claim 3

'058 Patent Claim 3	Disclosure
3. A computing system according to claim 1 wherein OSCSEs corresponding to and capable of performing the same function as SLCSEs remain in the operating system kernel.	<p>Choo, as evidenced by the example citations below, discloses the computing system according to claim 1 wherein OSCSEs corresponding to and capable of performing the same function as SLCSEs remain in the operating system kernel.</p> <p>This element is satisfied by the disclosure set forth at claim element 1[c], [d][1]-[2].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.</p>

Chart B-18

Invalidity Contentions: Choo

Claim 4

'058 Patent Claim 4	Disclosure
4. A computing system according to claim 1 wherein the one or more SLCSEs provided to one of the plurality of software applications having exclusive use thereof, use system calls to access services in the operating system kernel.	<p>Choo, as evidenced by the example citations below, discloses the computing system according to claim 1 wherein the one or more SLCSEs provided to one of the plurality of software applications having exclusive use thereof, use system calls to access services in the operating system kernel.</p> <p>This element is satisfied by the disclosure set forth at claim element 1[c], [d][1].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.</p>

Chart B-18

Invalidity Contentions: Choo

Claim 18

'058 Patent Claim 18	Disclosure
18. A computer system as defined in claim 2 wherein SLCSEs are not copies of OSCSEs.	<p>Choo, as evidenced by the example citations below, discloses the computer system as defined in claim 2 wherein SLCSEs are not copies of OSCSEs.</p> <p>This element is satisfied by the disclosure set forth at claim element 1[c], [d][1].</p> <p>To the extent Plaintiff contends that this reference does not disclose this limitation, the limitation would have been obvious to a person of ordinary skill in the art based on this reference either alone or in combination with (1) the general knowledge of one of ordinary skill in the art, and/or (2) the teachings of the prior art references set forth in Defendant's other invalidity charts for the '058 patent with respect to this limitation, as described in Defendant's Invalidity Contentions.</p>